



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,092	12/23/2003	Akira Suzuki	246897US2	8963
22850 7590 11/27/2007 OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C. 1940 DUKE STREET ALEXANDRIA, VA 22314			EXAMINER WANG, HARRIS C	
			ART UNIT 2139	PAPER NUMBER
			NOTIFICATION DATE 11/27/2007	DELIVERY MODE ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary

Application No.

10/743,092

Applicant(s)

SUZUKI ET AL.

Examiner

Harris C. Wang

Art Unit

2139

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5 and 7-137 is/are pending in the application.
- 4a) Of the above claim(s) See Continuation Sheet is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5, 10, 11, 25, 27, 32, 41-69, 105-114 and 129-131 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 December 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Continuation of Disposition of Claims: Claims withdrawn from consideration are 7-9,12-24,26,28-31,33-40,70-104,115-128 and 132-137.

DETAILED ACTION

Response to Arguments

In page 45 of Remarks, the Applicant has argued that "the Applicant's point to page 64, lines 14-16 of the present application which describe that 'a method of computing the feature amount is known in the electronic signature art.'

However this does not overcome the original indefinite rejection regarding the term "feature amount." The Applicant has not explained what exactly a "feature amount" is. Therefore the rejection of Claims 41-69 is repeated.

Applicant's arguments with respect to claim Claims 1-4, 10, 24, 32-41-46, 48-51, and 53-54 have been considered but are moot in view of the new ground(s) of rejection.

Regarding Claim 129, the Applicant argues that Miyazaki does not teach "a limitation cancellation program for canceling a limitation in the operation process of said operation processing program (pg. 48)." Applicant then writes "after receiving the execution verify logic conversion software, the user applies the execution verify logic conversion software to the trial-use encapsulated contents and this enables the actual use encapsulated contents to be installed" (pg. 48).

The Examiner interprets removing the trial version limitations as "cancelling a limitation."

The Applicant further argues that execution verify logic is not in an "encapsulated document structure (pg. 49 of Remarks)." The Examiner points to Figure 6 of Miyazaki that clearly shows that "execution verify logic" is in the "contents encapsulation means."

On page 50 of the Remarks, the Applicant argues that "Claim 55 retains an encrypted feature amount regarding the operation file, not a feature amount regarding the document structure." Later the Applicant writes "the signature key in Dray is not "a feature amount regarding said operation program file" (the operation file being a component of the encapsulated document structure) but rather a private signature key of a self signing signature document object (the entire structure."

Because the Applicant admits that the operation file is a component of the encapsulated document structure, the Examiner interprets that a feature amount "regarding" the document structure is also concerned with the program file contained inside.

On page 52 of the Remarks, the Applicant argues that "while the Office Action states that it would have been obvious to include an operating program outside of the document, the reason appears to be based on impermissible hindsight reconstruction."

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only

knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

In particular the Examiner believes that one of ordinary skill in the art would be able to store a program outside of a document. If the Applicant believes that the instant application stores a program outside of a document in a different manner than what is normally done, clarification is requested. Otherwise, if the application merely teaches that a program is stored outside a document, the Examiner maintains that one of ordinary skill would be able to store a program outside of a document.

The Applicant then argues, on Page 54 of Remarks, that "In Miyazaki, there is not a plurality of operating programs contained in the electronic document file...Assuming arguendo, that the first verify logic in Miyazaki is equivalent to Applicants' "operating programs" Miyazaki does not describe that the encapsulated contents include a plurality of first execution verify logic"

In the cited Paragraph[0049] of Miyazaki, the disclosure describes "The first execution verify logic consists of codes for controlling reference and execution operations in the course of displaying initial messages at a start, verifying the current digital contents, and making decisions of a user ID, machine ID or date and time." The Examiner interprets the "codes" that perform the various described functions as a "plurality" of operating programs.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 25, 41-69, 106, 108, 129 and 131 are rejected under 35

U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Each of these claims either claim or depend on a claim which recites the term "feature amount." The term "feature amount" is not well known in the art and is considered indefinite.

In particular in Claims 51-54, and Claims 65-69 teach "a feature amount regarding the operating program file...stored outside said single document." It is unclear what a "feature amount" actually is. The term "regarding the operation program file" is not clear in precisely how the feature amount relates to the document itself.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35

U.S.C. 102 that form the basis for the rejections under this section made in this

Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims rejected under 35 U.S.C. 102(b) as being anticipated by Dray (US 20020184485).

Regarding Claim 1,

Dray teaches an encapsulated document structure comprising:

a document information file storing document information that is a substance of expression of a document and an operating program file storing an operating program that materializes the document information, a limitation being given to the operating program by a security function when the operating program is interpreted and executed by a computer, (*"According to the present invention, a method is provided for creating, Self-Encrypting/decrypting Electronic Document Objects (SEDOs) that contain an embedded Cipher Management Program (CMP)" Paragraph [0082]*) The Examiner interprets that a document object inherently contains a document file.

Dray further teaches wherein the document information file and the operating program file are encapsulated as a single document. (*"The encryption and decryption processes are encapsulated within the SEDOs" Paragraph [0082]*)

Dray further teaches wherein said operating program is initiated by an external start program (*"The invention can be employed as..."macros" provided within other application programs, such as Microsoft Word" Paragraph [0034]*) (*"SEDO objects*

can be processed by any application program that understands the standard document representation language of a SEDO" Paragraph [0022]) The Examiner interprets "processing" the SEDO as initiating the operating program.

Regarding Claim 2,

Dray further teaches the encapsulated document structure as claimed in claim 1, wherein the security function of said operating program file is controlled based on specific decryption key information for decrypting encrypted digital information. (*"The CMP then retrieves the ciphertext component of the E-SEDO, obtains the symmetric key needed to decrypt the ciphertext component using a secure protocol, and decrypts the ciphertext to produce plaintext" Paragraph 0115])*

Regarding Claims 3 and 4,

Dray teaches the encapsulated document structure as claimed in claim 2, further comprising encapsulating means for encapsulating said decryption key information, said operating program file and said document information file into a single document. (*"According to the present invention, a method is provided for creating, Self-Encrypting/decrypting Electronic Document Objects (SEDOs) that contain an embedded Cipher Management Program (CMP) The encryption and decryption processes are encapsulated within the SEDOs" Paragraph [0082]). It is inherent that a decrypting process has decryption key information.*

Regarding Claim 10,

Dray teaches the encapsulated document structure as claimed in claim 3, where decryption key information includes link information of URL. (*"Employing the signature algorithm embedded in the encoded message, or downloaded from a Web site the address of which (i.e. the URL of which) is embedded in the encoded message"* Paragraph [0048])

Regarding Claims 25 and 32,

Dray teaches the encapsulated document structure as claimed in claim 1, wherein said contents information file includes:

at least one contents file that serves as a substance of expression on a document; (It is inherent that a document object has at least a substance of expression)

and a document structure file specifying a structure of the contents file and a display status on said document. (*"Collecting the elements of the host document*

into a data structure that represents the canonical form of the document at the time signature, that is, arranging the elements of the document object in a defined common format, in order that the Cipher Management Program...will be able reliably to decompose the document into a consistent data structure for processing" Paragraph [0040]). The Examiner interprets the display status as the common format for which the document will be displayed.

It is inherent that the encryption/decryption program is provided with a minimum unit necessary to process the contents file.

Regarding Claims 41 and 42,

Dray teaches the encapsulated document structure as claimed in claim 1, further comprising a feature amount retaining file retaining an encrypted feature amount regarding said program file, the feature amount retaining file being encapsulated into said single file.

The Examiner interprets "feature amount retaining file" as the electronic signature file of the document structure. (*"The embedded signature program decomposes the data structure representing the P-SSDO into a linear sequence of bits, as required by electronic signature algorithms, and retrieves the user's private signature key. The bit sequence and signature are then passed to an appropriate signature algorithm...which generates and returns an electronic signature."* Paragraph [0061]) (*"The electronic signature is stored along with the S-SSDO for subsequent verification"* Paragraph [0062])

Dray teaches decomposing “the data structure representing the P-SSDO into a linear sequence of bits” which the Examiner interprets as generating the signature for both the document file as well as the program file.

Regarding Claim 43,

Dray teaches the encapsulated document structure as claimed in claim 41, wherein said feature amount retaining file retains decryption key information used for decrypting the encrypted feature amount regarding said operating program file.

The Examiner interprets retaining “decryption key information used for decryption the encrypted feature amount regarding said operation file” as retaining the private key information used to generate the digital signature of the document.

(“The bit sequence and [private] signature key are then passed to an appropriate signature algorithm...the signature algorithm may be an integral part of the signature processing program embedded in the P-SSDO” Paragraph [0061])

Regarding Claim 44,

Dray teaches the encapsulated document structure as claimed in claim 41, wherein said feature amount retaining file retains location information which indicates decryption key information used for decrypting the encrypted feature amount regarding said operating program file. (*"Employing the signature algorithm embedded in the encoded message, or downloaded from a Web site the address of which (i.e. the URL of which) is embedded in the encoded message" Paragraph [0048]*) The Examiner interprets location information as the destination address (URL).

Regarding Claim 45,

Dray teaches the encapsulated document structure as claimed in claim 43, wherein a different set of said decryption key information is related to each operating program file. (*"The existing public key scheme described above requires that a public/private key pair be generated for each user during the initial registration process" Paragraph [0069]*)

Regarding Claim 46,

Dray teaches the encapsulated document structure as claimed in claim 44, wherein a different set of said decryption key information is related to each operating program file. (*"The existing public key scheme described above requires*

that a public/private key pair be generated for each user during the initial registration process" Paragraph [0069])

Regarding Claim 48,

Dray teaches the encapsulated document structure as claimed in claim 43, wherein said decryption key information is signed and encrypted by a third party authority (*"by obtaining the public key of the CA that signed the user's certificate and verifying the CA's signature on the certificate, as indicated above, and extracts the user's public key from the CA's certificate data base" Paragraph [0077])*).

Regarding Claim 49,

Dray teaches the encapsulated document structure as claimed in claim 41, wherein the feature amount regarding said operating program file is encrypted by a private key encryption method. (*"The bit sequence and [private] signature key are then passed to an appropriate signature algorithm...which generates and returns an electronic signature" Paragraph [0061])*

Regarding Claim 50,

Dray teaches the encapsulated document structure as claimed in claim 41, further comprising a feature amount verification program for performing a verification of a tamper on said operating program file, the feature amount verification program being encapsulated into said file. (*"This event executes the signature verification program embedded in the S-SSDO...The bit sequence, signature data, and signer's public key material are then used to verify the origin and structural integrity of the P-SSDO" Paragraph [0064]*)

Regarding Claims 51 and 53,

Dray teaches the encapsulated document structure as claimed in claim 1, wherein a feature amount of the operating program in said operating program file is stored outside said single document is encrypted by a private key encryption method. (*"A signature program may be physically embedded within the host document, or may be an external program file that is executed through a link within the document" Paragraph [0037]*) (*"The bit sequence and [private] signature key are then passed to an appropriate signature algorithm...which generates and returns an electronic signature" Paragraph [0061]*)

Regarding Claim 54,

Dray teaches the encapsulated document structure as claimed in claim 51, further comprising a feature amount verification program for performing a verification of a tamper on said operating program file, the feature amount verification program being encapsulated into said file. (*"This event executes the signature verification program embedded in the S-SSDO...The bit sequence, signature data, and signer's public key material are then used to verify the origin and structural integrity of the P-SSDO" Paragraph [0064]*)

Claims 129-130 are rejected under 35 U.S.C. 102(b) as being anticipated by Miyazaki (US 20010044780).

Regarding Claim 129,

Miyazaki teaches an encapsulated document structure, comprising:

contents information that is a substance of expression (*Figure 2, Digital Contents*);

an operating program read by an accessing-side computer connected to a network, the operating program causing the accessing-side computer to perform various functions (*Figure 2. First Execution Verify Logic*);

and wherein said operating program includes: an operation processing program of which operation process on said contents information is limited based on authority information; (*"This enables the encapsulated contents including the first execution verify logic to be distributed as a trial-use digital contents whose operations is restricted"* (Paragraph [0059])

and a limitation cancellation program for canceling a limitation in the operation process of said operation processing program by sending various kinds of information based on said sending location information, where sending location information is for sending various kinds of information to a providing-side computer connected to said through said network (*"Here, the second execution verify logic may have less severe execution restrictions than the first execution verify logic"* Paragraph [0019]) (*"the logic to implement such a function and the destination address are placed into the specifications of the second execution verify logic. Third, the specifications are transmitted to the copyright management agency through the information transmission medium"* Paragraph [0130]). The Examiner interprets the destination address as "sending location information."

wherein said contents information, said operating program and said sending location information are encapsulated into a single document. (*Figure 2 shows the contents encapsulated with an operating program. After the verification*

conversion, the second executions verify logic replaces the first, therefore encapsulating the content, operating program and sending location information.)

Miyazaki teaches that digital content may include "text" which the Examiner interprets as an electronic document.

Regarding Claim 130,

Miyazaki teaches the encapsulated document structure as claimed in claim 129, wherein said contents information is encrypted, and said limitation cancellation program acquires decryption key information for decrypting the encrypted contents document based on said sending location information through said network so as to decrypt the encrypted contents information based on the decryption key information acquired. (*"the decryption of the encrypted digital contents is carried out as follows: First, the private key acquisition means acquires the user's private key from the private key storage means in the user terminal; second, the contents key stored in the contents key storage means is decrypted using the private key; and then the digital contents in the encapsulated contents are decrypted using the content key"* Paragraph [0114])

The Examiner interprets the decryption key information for decrypting the encrypted contents as the private key. It is inherent that the destination address (sending location information) must be sent in order to properly receive the decryption key information.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 5, 47 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dray (US 20020184485).

Regarding Claim 5, (103 Dray)

Dray teaches the encapsulated document structure as claimed in claim 3. Dray teaches decryption key information encrypted. Dray also teaches using a third party authority to certify a user. (*"In response, the CA creates a public key certificate for the user, signs the certificate with the private key of the CA and stores the signed certificate in a publicly accessible certificate database"* Paragraph [0069])

However Dray does not explicitly teach wherein said decryption key information is signed and encrypted by a third party authority.

It would have been obvious to one of ordinary skill in the art at the time of the invention to use a third party to sign and encrypt decryption key information.

The motivation is that Dray already teaches encrypting the decryption key information, and furthermore already teaches using a 3rd party to certify. One of ordinary skill would be able to use the third party to encrypt and sign decryption key information.

Regarding Claim 47, (Dray 103)

Dray teaches the encapsulated document structure as claimed in claim 41. However Dray does not explicitly teach wherein the feature amount regarding said operating program file is encrypted by a public key encryption method.

Dray does teach the signature is encrypted by private key encryption "*The bit sequence and [private] signature key are then passed to an appropriate signature algorithm...which generates and returns an electronic signature*" Paragraph [0061])

It would have been obvious to one of ordinary skill in the art at the time of the invention to encrypt the signature using a public key.

The motivation is public key encryption is well known in the art.

Regarding Claims 52,

Dray teaches the encapsulated document structure as claimed in claim 51 wherein said feature amount of operating program file that is stored outside the document is encrypted by a public key encryption method.

It would have been obvious to one of ordinary skill in the art at the time of the invention to encrypt an operating program outside of the document with a public key.

The motivation is that because public key encryption are well known in the art so one of ordinary skill in the art would be able to encrypt a program outside of a document with these well known techniques.

Claims 11, 55-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dray in view of Raman (6249794).

Regarding Claim 11,

Dray teaches the encapsulated document structure as claimed in Claim 3. However Dray does not explicitly teach wherein a storage area of said operating program is described therein.

Raman teaches a "document description format (DDF) file [that] encapsulates the location of a document along with useful descriptive information about the document." (Column 2, lines 59-61)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the encapsulated document of Dray with the DDF file of Raman.

The motivation is that encapsulating description of storage information in a document is well known in the art.

Regarding Claims 55 and 56,

Dray teaches an encapsulated document structure comprising:

a document information file storing contents information that is a substance of expression on a document; (It is inherent that a Document Object has at least a substance of expression)

and a feature amount retaining file retaining an encrypted feature amount regarding said operating program file, where The Examiner interprets "feature amount retaining file" as the electronic signature file of the document structure.

("The embedded signature program decomposes the data structure representing the P-SSDO into a linear sequence of bits, as required by electronic signature algorithms, and retrieves the user's private signature key. The bit sequence and signature are then passed to an appropriate signature algorithm...which generates and returns an electronic signature." Paragraph [0061])

wherein said document information file, and said feature amount retaining file, and other information are encapsulated into a single file. *("The electronic signature is stored along with the S-SSDO for subsequent verification" Paragraph [0062])*

Dray teaches decomposing "the data structure representing the P-SSDO into a linear sequence of bits" which the Examiner interprets as generating the signature for both the document file as well as the program file.

Dray does not explicitly teach location information indicating a location where an operating program file is stored, the operating program file storing an operating program for materializing the document information file.

Raman teaches a "document description format (DDF) file [that] encapsulates the location of a document along with useful descriptive information about the document." (Column 2, lines 59-61)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the encapsulated document of Dray with the DDF file of Raman.

The motivation is that location information may be included as information facilitating secure access to the secured file.

Regarding Claim 57,

Dray and Raman teach the encapsulated document structure as claimed in claim 55, wherein said feature amount retaining file retains decryption key information used for decrypting the encrypted feature amount regarding said operating program file.

The Examiner interprets retaining "decryption key information used for decryption the encrypted feature amount regarding said operation file" as retaining the private key information used to generate the digital signature of the document.

("The bit sequence and [private] signature key are then passed to an appropriate signature algorithm...the signature algorithm may be an integral part of the signature processing program embedded in the P-SSDO" Paragraph [0061])

Regarding Claim 58,

Dray and Raman the encapsulated document structure as claimed in claim 55, wherein said feature amount retaining file retains location information

which indicates decryption key information used for decrypting the encrypted feature amount

regarding said operating program file. (*"Employing the signature algorithm embedded in the encoded message, or downloaded from a Web site the address of which (i.e. the URL of which) is embedded in the encoded message" Paragraph [0048]*)
The Examiner interprets location information as the destination address (URL).

Regarding Claim 59,

Dray and Raman teach the encapsulated document structure as claimed in claim 57, wherein a different set of said decryption key information is related to each operating program file. (*"The existing public key scheme described above requires that a public/private key pair be generated for each user during the initial registration process" Paragraph [0069]*)

Regarding Claim 60,

Dray and Raman he encapsulated document structure as claimed in claim 58, wherein a different set of said decryption key information is related to each operating program file. (*"The existing public key scheme described above requires that a public/private key pair be generated for each user during the initial registration process" Paragraph [0069]*)

Regarding Claim 61,

Dray and Raman teach the encapsulated document structure as claimed in claim 55.

Dray and Raman do not teach wherein the feature amount regarding said operating program file is encrypted by a public key encryption method.

Dray does teach the signature is encrypted by private key encryption (*"The bit sequence and signature key are then passed to an appropriate signature algorithm...which generates and returns an electronic signature" Paragraph [0061]*)

It would have been obvious to one of ordinary skill in the art at the time of the invention to encrypt the signature using a public key.

The motivation is public key encryption is well known in the art.

Regarding Claim 62,

Dray and Raman teach the encapsulated document structure as claimed in claim 57, wherein said decryption key information is signed and encrypted by a third party authority. (*"by obtaining the public key of the CA that signed the user's certificate and verifying the CA's signature on the certificate, as indicated above, and extracts the user's public key from the CA's certificate data base" Paragraph [0077]*).

Regarding Claim 63,

Dray and Raman teach the encapsulated document structure as claimed in claim 55, wherein the operating program is encrypted by a private key encryption method. (*"The bit sequence and [private] signature key are then passed to an appropriate signature algorithm...which generates and returns an electronic signature" Paragraph [0061])*)

Regarding Claim 64,

Dray and Raman teach the encapsulated document structure as claimed in claim 55, further comprising a feature amount verification program for performing a verification of a tamper on said operating program file, the feature amount verification program being encapsulated into said file. (*"This event executes the signature verification program embedded in the S-SSDO...The bit sequence, signature data, and signer's public key material are then used to verify the origin and structural integrity of the P-SSDO" Paragraph [0064])*)

Regarding Claim 65,

Dray teaches an encapsulated document structure comprising:

a document information file storing contents information that is a substance of expression on a document; (*Figure 9. Encrypted Data, 924*)

and a feature amount retaining file retaining an encrypted feature amount regarding said operating program file, (*Figure 9. Encrypted Security Information, 926*)

wherein said document information file, and said feature amount retaining file, and other information are encapsulated into a single file. (Figure 9)

Dray does not explicitly teach location information indicating a location where an operating program file is stored, the operating program file storing an operating program for materializing the document information file.

Raman teaches a "document description format (DDF) file [that] encapsulates the location of a document along with useful descriptive information about the document." (Column 2, lines 59-61)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the encapsulated document of Dray with the DDF file of Raman.

The motivation is that location information may be included as information facilitating secure access to the secured file.

The cited portions of the combined references do not explicitly teach a feature amount regarding the operating program file is stored outside said single file.

It would have been obvious to one of ordinary skill in the art at the time of the invention to include an operating program outside of the document.

The motivation is that one of ordinary skill in the art would be able to store a program outside of a document.

Regarding Claims 66 and 68,

Dray and Raman teaches the encapsulated document structure as claimed in claim 65, wherein a feature amount of the operating program in said operating program file is stored outside said single document is encrypted by a private key encryption method. (*"A signature program may be physically embedded within the host document, or may be an external program file that is executed through a link within the document" Paragraph [0037]*) (*"The bit sequence and [private] signature key are then passed to an appropriate signature algorithm...which generates and returns an electronic signature" Paragraph [0061]*)

Regarding Claim 67,

Dray and Raman teaches the encapsulated document structure as claimed in claim 65 wherein said feature amount of operating program file that is stored outside the document is encrypted by a public key encryption method.

It would have been obvious to one of ordinary skill in the art at the time of the invention to encrypt an operating program outside of the document with a public key.

The motivation is that because public key encryption are well known in the art so one of ordinary skill in the art would be able to encrypt a program outside of a document with these well known techniques.

Regarding Claim 69,

Dray and Raman teach the encapsulated document structure as claimed in claim 65, further comprising a feature amount verification program for performing a verification of a tamper on said operating program file, the feature amount verification program being encapsulated into said file. (*"This event executes the signature verification program embedded in the S-SSDO...The bit sequence, signature data, and signer's public key material are then used to verify the origin and structural integrity of the P-SSDO"* Paragraph [0064])

Claim 27 is rejected under 35 U.S.C. 103(a) as being unpatentable over Dray in view of Wagner (US 20040006562).

Regarding Claim 27,

Dray teaches the encapsulated document structure as claimed in claim 25. Dray does not further teach comprising a library file storing said contents file with an index indicating a storing location thereof, wherein said operating program file specifies said contents file according to said index.

Wagner teaches a "request system [that] will receive document requests from user 10 and use location information in database 24 of library system 20 to generate input file 16 in hit list format...the query format comprises index values that are used to build one or more query strings." Paragraph [0028])

It would have been obvious to one of ordinary skill in the art at the time of the invention to add a library file storing contents file indicating the storage location of the content to the encapsulated document of Dray.

The motivation is that using library files to store content and having an index indicating the storing location is well known in the art.

Claim 131 is rejected under 35 U.S.C. 103(a) as being unpatentable over Miyazaki (US 20010044780).

Regarding Claim 131,

Miyazaki teaches the encapsulated document structure as claimed in claim 130, wherein decryption key request information is encapsulated into said single document together with said contents information, said operating program and said sending location information, *(Figure 11 shows the Second Execution Verify Means, which contains sending location information, the Examiner interprets "decryption key request information" as Private Key Acquisition Means. After the verification conversion, the second executions verify logic replaces the first, therefore encapsulating the content, operating program, sending location information and decryption key request information)*

the decryption key request information for requesting said providing-side computer to send decryption key information necessary for acquiring said decryption key information, and said limitation cancellation program includes:

a decryption key information requesting program for requesting said decryption key information by sending said decryption key producing information request information to said providing-side computer through said network based on said sending location information; decryption key information reception program for receiving said decryption key information from said providing-side computer through said network; *(Figure 11, Private Key Acquisition Means)*. The Examiner interprets the act of acquiring as requesting and receiving.

and a decryption program for decrypting the encrypted contents information based on said decryption key information produced by said

decryption key producing program. (*"the contents key...is decrypted using the private key" Paragraph [0114]*). *This inherently requires a decryption program.*

However Miyazaki does not explicitly teach requesting decryption key producing information or a decryption key program for producing said decryption key information based on said decryption key information received by said decryption key information reception program;

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the decryption key acquiring method of Miyazaki with a decryption key producing program.

The motivation is the end result is the same, where a decryption key is received to decrypt encrypted content. One of ordinary skill in the art would be able to produce a decryption key if given the proper information.

Claims 105-112, 114 are rejected under 35 U.S.C. 103(a) as being unpatentable over Miyazaki in view of in view of Anderson (6021202).

Regarding Claims 105-112, 114

Miyazaki teaches an encapsulated file comprising:

a plurality of operating programs and operating program use information provided by an operating program provider; and a contents file and contents

use information produced by said operating program provider or a document producer. (*"digital contents include, for example, images, motion pictures, voice, text, software or their combinations"* Paragraph [0049]).

one of said operating programs is an verification program that operates other operating programs based on said operating program use information. (*"In Fig. 2, the reference numeral 6 designates encapsulated contents; 7 designates a first execution verify logic that provides execution verify means for carrying out execution control and verification of the digital contents"* Paragraph [0048])

Miyazaki further teaches a verification program that verifies a tamper on digital content. (*Figure 8, Digital Signature Verify Means, 31*)

Miyazaki further teaches a verification program that limits use of digital content. (*"This enables the encapsulated contents including the first execution verify logic to be distributed as a trial-use digital contents whose operation is restricted"* Paragraph [0059])

Miyazaki does not explicitly teach that the encapsulated contents are a document file.

Anderson teaches an "electronic document [that] is made up of a number of blocks as depicted in FIGS. 31-34. (*Column 19, Lines 22-23*). Anderson further teaches "whenever a block is to be authenticated, or tamper-proofed, a digital signature block is added to the electronic document. The signature block contains a reference to a certificate block containing a public key used to verify the digital signature." (*Column 20, lines 62-66*)

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the encapsulated digital contents and execution verification of Miyazaki with the tamper-proofed document of Anderson.

The motivation to combine the inventions of Miyazaki and Anderson is that the digital content of Miyazaki includes text, which one of ordinary skill could interpret as an electronic document. Furthermore Miyazaki teaches that encapsulating digital content with a verification program is well known in the art.

Because the encapsulated digital content of Miyazaki contains both operating programs as well as a contents file, the Examiner interprets the content verification program and the operation verification program as the same program.

Claim 113 rejected under 35 U.S.C. 103(a) as being unpatentable over Miyazaki in view of Anderson as applied to claim 106 above, and further in view of Hidalgo (US 20030313).

Regarding Claim 113,

Miyazaki and Anderson teach the electronic document file as claimed in claim 106.

Miyazaki and Anderson do not explicitly teach wherein, when safety of said operating programs is not guaranteed by said operation verification

program, a user of said electronic document file is notified of the fact that safety of said operating programs is not guaranteed.

Hidalgo teaches "If the system 20 finds that an attempt to tamper the parameters occurred, the system 20 sends an error message to the user, logs the illegal access attempt, and optionally relays the error to the administrator" (Paragraph [0135])

It would have been obvious to one of ordinary skill in the art at the time of the invention to alert a user when the a tamper has occurred.

The motivation is that notifying a user that a tamper has occurred (safety is not guaranteed) is a well known way of responding to a tamper.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will

the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harris C. Wang whose telephone number is 5712701462. The examiner can normally be reached on M-F 8-5:30, Alternate Fridays Off.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ R. SHEIKH can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number:
10/743,092
Art Unit: 2139

Page 36

HCW


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100